Assessment and Authorization– Module 5 (combined with Module 6)

ELO-120 List the DoD information impact levels, and provide an example of each type.

ELO-130 Identify issues associated with storing DoD data in non-US locations.

ELO-150 Identify risks associated with using outsourced IT offerings.

ELO-160 Match key risk terms from the section to appropriate definitions.

Module – 5: Assessment and Authorization

Topics

- Security Assessment and Authorization Overview
- Accreditation Process for Externally-Provided CSO
- The DoD Information Impact Levels
- Federal Risk and Authorization Management Program
- FedRAMP Security Process
- DOD Provisional Authorization
- DoD Provisional Authorization Process
- Cloud Access Point
- Authorizing Official Tasks
- Security A&A Risk Terms
- Module Review
- Module Summary Questions

You should be able to:

- List the DoD information impact levels, and provide an example of each type.
- Identify issues associated with storing DoD data in non-US locations.
- Identify risks associated with using outsourced IT offerings.
- Match key risk terms from the section to appropriate definitions.

Security A&A Overview

Topic

Security Assessment Overview

You should be able to:

To describe the high level assessment and authorization steps required for a cloud solution.

Questions

RMF - Major System Security Lifecycle Steps

1. Categorize System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize System
6. Monitor Security Controls

Content

- To address the cloud IT security risks identified in the previous module a Component implements security controls based on the risk assessment of the threats and conducts a security assessment and accreditation in accordance with the DoD Risk Management Framework (RMF)
- The DoD RMF is described in DoDI 8510.01 and provides the overall policy regarding the security of DoD Information Systems.
- **The most important part of this policy is that the DoD Component appoints a trained Authorizing Official (AO) to oversee the process and who provides the final Approval to Operate (ATO) the cloud service when he/she feels the security risks of the CSO have been appropriately addressed**
- Another important component is cybersecurity reciprocity.
- According to DoDI 8510.01, "Cybersecurity reciprocity is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation."

Security A&A Overview (Continued)

Topic

Security Assessment Overview (continued)

You should be able to:

Questions

Content

- To reduce the duplication of effort in assessing Cloud Service Offerings (CSO), the DOD leverages the GSA Federal Risk and Authorization Management Program (FedRAMP) and DISA Provisional Authorization (PA) processes detailed in the Cloud Computing SRG to share security assessments among federal agencies.
- In procuring cloud services, it is important that the AO and acquisition professional work with the organization's security team to determine the information impact level of the data that will be required to be processed by the CSO.
- The impact level will determine the process that will be used to procure the cloud services and the cloud service offerings that are eligible to meet the organization's IT requirements.
- Note the focus is on the cloud service offering not with the cloud provider of the service who may offer services that are certified at different information impact levels.
- If the required CSO will be operating at Information Impact Level 4 or above, then the CSO will need a Cloud Access Point (CAP) solution for connecting to the NIPRNET.

Accreditation Process for Externally-Provided CSO

Topic

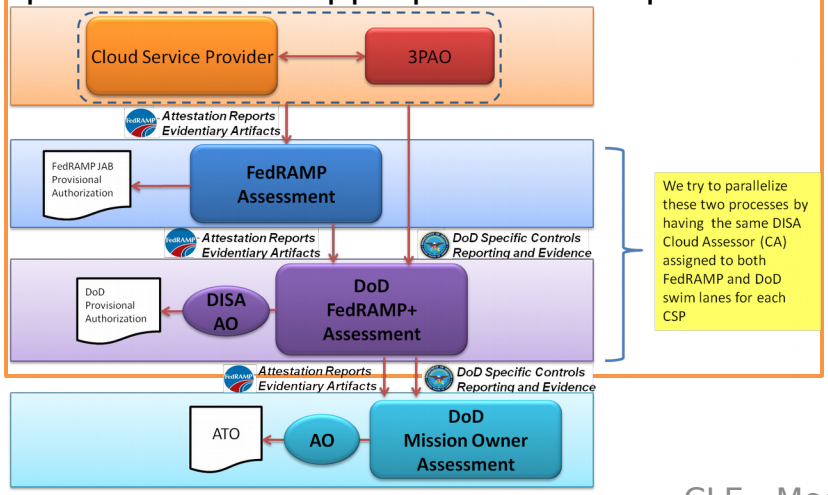
Accreditation Process for Externally-Provided CSO

You should be able to:

Identify the 7 steps in performing an assessment

Questions

Match the 7 steps of the assessment process to the appropriate description



Content

- The six step RMF security assessment and accreditation steps are modified to leverage the FedRAMP and DoD Provisional Assessment processes
- Determine Information Impact Level – determine the Information Impact Level of the application/system to be procured in accordance with the DoD Cloud Computing Security Requirements Guide (SRG)
- Select Cloud Service Offering (CSO) – select the appropriate CSO based on the functional requirements and the Impact Level either from the DoD Approved Cloud Service Provider Catalog, FedRAMP Compliant Systems with Joint Authorization Board (JAB) approval, compliant cloud systems with an Agency FedRAMP Authorization, or by Component approved selection process
- Initiate Assessment Process– contact DISA Cloud Support Office to request Provisional Authorization (PA) of your Component's use of the CSO, work with the CSP to complete the appropriate DISA forms, and submit them.
- Conduct Security Testing and Assessment – determine what FedRAMP or DoD security assessments have been conducted for the CSO, and either have a 3rd Party Assessment Organization (3PAO) or have DoD conduct security testing and assessment in accordance with the SRG, if an assessment has NOT already been completed by an authorized 3PAO or DoD organization or if these assessments are considered insufficient for this Component's security needs
- Support DISA Provisional Authorization – submit assessment information to DISA and work with DISA to mitigate any issues identified that will need be addressed to obtain a DISA PA from the DISA Approving Official (AO)
- Prepare Component Security Authorization Package (SAP) – after obtaining DISA PA, conduct security assessment and risk analysis in accordance with the Component's security

The DoD Information Impact Levels

Topic

Security Information Impact Levels

You should be able to:

1. Know the 4 DoD security impact levels and provide an example of each one
2. Identify the high level security controls for each level
3. Identify which impact levels require a Cloud Access Point?

Questions

1. What are the 4 impact levels?
2. Provide an example of data at each impact level
3. For which impact levels is a CAP required?
4. Which level requires a classified security controls overlay?
5. Which level requires only FedRAMP Moderate controls?

Content

- The Cloud Computing Security Requirements Guide (SRG) describes 4 impact levels
- Level 2 Information Impact Level is for public data/non-sensitive data, e.g. DoD news and organization information for non-DoD individuals
- Level 4 Information Impact Level is for critical mission information, e.g. personally identifiable information (PII) or Protected Health Information (PHI)
- Level 5 information impact level is for high sensitivity National Security Systems, e.g. unclassified mission information that is more sensitive than Level 4
- Level 6 information impact level is for classified SECRET National Security Systems
- Level 2 systems require FedRAMP Moderate controls
- Level 4 systems requires Level 2 controls and Level 4 overlay of controls
- Level 5 requires Level 4 controls plus controls for National Security Systems and other controls required for level 5
- Level 6 requires Level 5 controls plus classified security controls; however Level 6 cloud services are not the focus of this training, so it will not be discussed in any detail
- Level 4 systems and above require a DoD Cloud Access Point (CAP) between the system and the

Information Impact Level 2

Topic

Information Impact Level 2

You should be able to:

Questions

Content

- Information Impact Level 2 data is DOD data that the Component cleared for public release, information that has gone through the Freedom of Information Act (FOIA) process for release, information open to the public even if it requires a login.
- Level 2 applies to non-National Security Systems (NSS) only.
- The Deployment Model can be a Public Cloud
- For Level 2 data the Component can use a cloud service offering that has:
  - Properly implemented the General Services Administration (GSA) FedRAMP Version 2 Moderate security controls that have validated by either a FedRAMP certified 3PAO or a DoD ATO and has the approval of the Joint Authorization Board (FedRAMP).
  - The system also requires a DOD PA. For Level 2 systems, no additional assessment is required for a DOD PA beyond the above FedRAMP approval process.
  - The CSP must maintain its FedRAMP approval for its CSO for the CSO to continue to have a DOD PA.
  - The Authorizing Official for the Component must also provide Authorization to Operate or Interim Authority to Test (IATT) before use of the cloud service
  - For Information Impact Level 2 there are no special connectivity requirements for accessing the CSO over the NIPRENET

Information Impact Level 4

Topic

Information Impact Level 4

You should be able to:

Questions

Content

- Information Impact Level 4 data includes Controlled Unclassified Information (CUI) (i.e., For Official Use Only (FOUO), Law Enforcement Sensitive (LES), DoD Unclassified Controlled Nuclear Information (DOD UCNI), and Limited Distribution)
- Information Impact Level 4 systems are considered non-National Security Systems (NSS).
- Some examples of CUI include:
  - Non-Appropriated Fund (NAF) data, educational systems that fall under The Family Educational Rights and Privacy Act (FERPA)
  - Moderate and Sensitive PII (social security numbers, alien ID and other immigration documents, passport numbers, driver's license numbers, vehicle identification numbers, and license plates)
  - Trade Secrets Act data
  - Protected Health Information (PHI) medical protected by the Health Insurance Portability and Accountability Act (HIPAA)
  - Legal
  - Law enforcement
  - Biometric data
- Eligible cloud service offerings are required to meet FedRAMP Version 2 Plus security controls, which contains additional security controls for the system beyond the controls specified in FedRAMP Version 2 Moderate guidance.
- DISA must approve these cloud offerings as a Level 4-cloud service through the PA process.
- System requires connection to the DoD Enterprise Cloud Access Point Solution (CAP) for connectivity to the DODIN
- This solution requires that the deployment model used is either DoD /Federal Government Tenants only Community Cloud or a Private Cloud

Information Impact Level 5

Topic

Information Impact Level 5

You should be able to:

Questions

Content

- Information Impact Level 5 systems include mission essential, critical infrastructure (military or civilian), deployment and troop movement, International Traffic in Arms Regulation (ITAR) data, or unclassified nuclear data.
- The system is considered a National Security System (NSS)
- Eligible cloud service offerings are required to meet FedRAMP Version 2 security controls plus additional security controls required for a Level 5 system
- DISA must approve them as a Level 5 cloud service through its PA process
- These systems requires a CAP solution
- This solution requires that the deployment model used is either DoD/Federal Government Tenants only Community Cloud or a Private Cloud

Federal Risk and Authorization Management Program

Topic

Federal Risk and Authorization Management Program (FedRAMP)

You should be able to:

Questions

Content

- FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- The Office of Management and Budget (OMB) mandated compliance with FedRAMP for all Federal Agencies as their systems and applications are migrated to the commercial cloud under the Federal Government's Cloud-First initiatives.
- OMB policy requires Federal departments and agencies to utilize FedRAMP approved CSP and share Agency Authorization to Operate (ATO) documentation with the FedRAMP Secure Repository.
- FedRAMP uses a "do once, use many times" framework designed to reduce cost, time, and staff required for security assessments and process monitoring reports.
- The FedRAMP Joint Authorization Board (JAB) is the primary governance and decision-making body for the FedRAMP program. JAB approved standards and processes result in the award and maintenance of a PA to host Federal Government missions.

FedRAMP Security Process

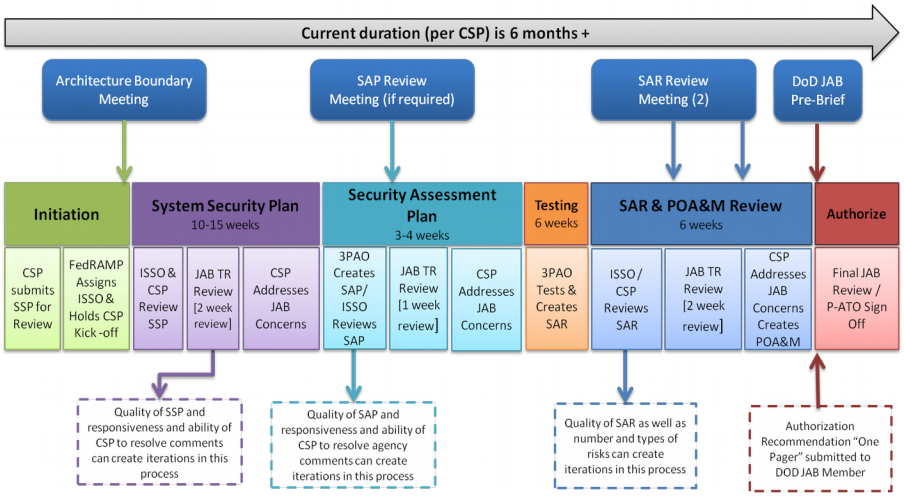
Topic

FedRAMP Security Process

You should be able to:

1. Identify the 6 steps of the FedRAMP Process

Questions


Current duration (per CSP) is 6 months +
Architecture Boundary Meeting
SAP Review Meeting (if required)
SAR Review Meeting (2)
DoD JAB Pre-Brief
Initiation
System Security Plan
10-15 weeks
Security Assessment Plan
3-4 weeks
Testing
6 weeks
SAR & POA&M Review
6 weeks
Authorize
CSP submits SSP for Review
FedRAMP Assigns ISSO & Holds CSP Kick-off
ISSO & CSP Review SSP
JAB TR Review [2 week review]
CSP Addresses JAB Concerns
3PAO Creates SAP/ ISSO Reviews SAP
JAB TR Review [1 week review]
CSP Addresses JAB Concerns
3PAO Tests & Creates SAR
ISSO / CSP Reviews SAR
JAB TR Review [2 week review]
CSP Addresses JAB Concerns Creates POA&M
Final JAB Review / P-ATO Sign Off
Quality of SSP and responsiveness and ability of CSP to resolve comments can create iterations in this process
Quality of SAP and responsiveness and ability of CSP to resolve agency comments can create iterations in this process
Quality of SAR as well as number and types of risks can create iterations in this process
Authorization Recommendation "One Pager" submitted to DOD JAB Member

Content

- Initiation
  - CSP submits System Security Plan (SSP)
  - FedRAMP assigns Information Systems Security Officer (ISSO) and holds kickoff
- System Security Plan Review
  - CSP and ISSO review SSP
  - JAB Technical Representative (TR) Review
  - CSP addresses JAB concerns
- Security Assessment Planning (SAP)
  - 3rd Party Assessment Organization (3PAO) creates SAP and ISSO reviews
  - JAB TR reviews SAP
  - CSP addresses JAB concerns
- Testing – 3PAO tests and creates Security Assessment Report (SAR)
- SAR Review Meeting
  - ISSO/CSP reviews SAR
  - JAB TR review
  - CSP addresses JAB concerns and creates Plan of action and Milestones (POAM)
- Authorize – Final JAB Review/P-ATO

DOD Provisional Authorization

Topic

DOD Provisional Authorization

You should be able to:

Questions

Content

- A DoD PA is an acceptance of risk based on an evaluation of the CSPs CSO and the potential for risk introduced to DOD networks. The DoD PA process follows the same “do once, use many times” framework as FedRAMP does.
- DoD PAs are granted at all information impact levels which provides a foundation that Authorizing Officials responsible for mission applications must leverage in determining the overall risk to the missions/applications that are executed as part of a CSO.
- A DoD PA is required for all CSOs
- The DISA Authorized Official for DOD PAs approves the requests for CSOs to receive a DOD PA after reviewing the documentation provided by the Mission Owner and the CSP through the DISA Direct Order Entry system and after reviewing the recommendations of the Defense Security Accreditation Working Group (DSAWG).

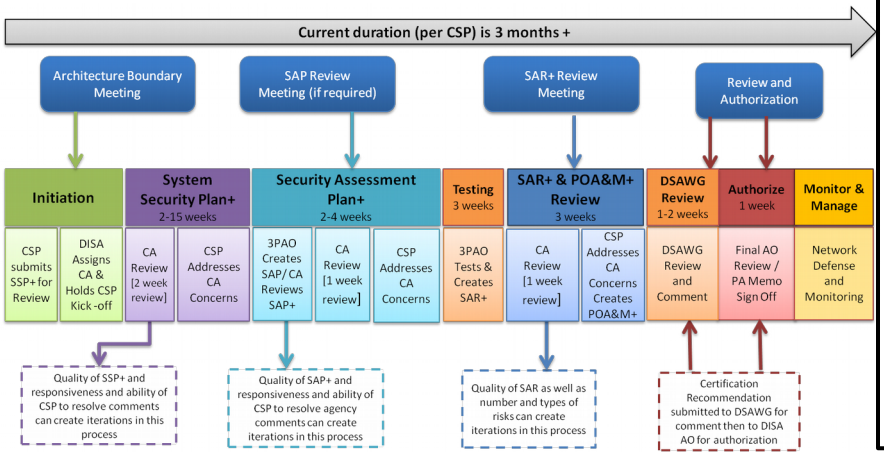
DoD Provisional Authorization Process

Topic

DoD Provisional Assessment

You should be able to:

Questions


Current duration (per CSP) is 3 months +
Architecture Boundary Meeting
SAP Review Meeting (if required)
SAR+ Review Meeting
Review and Authorization
Initiation
System Security Plan+ 2-15 weeks
Security Assessment Plan+ 2-4 weeks
Testing 3 weeks
SAR+ & POA&M+ Review 3 weeks
DSAWG Review 1-2 weeks
Authorize 1 week
Monitor & Manage
CSP submits SSP+ for Review
DISA Assigns CA & Holds CSP Kick-off
CA Review [2 week review]
CSP Addresses CA Concerns
3PAO Creates SAP/ CA Reviews SAP+
CA Review [1 week review]
CSP Addresses CA Concerns
3PAO Tests & Creates SAR+
CA Review [1 week review]
CSP Addresses CA Concerns Creates POA&M+
DSAWG Review and Comment
Final AO Review / PA Memo Sign Off
Network Defense and Monitoring
Quality of SSP+ and responsiveness and ability of CSP to resolve comments can create iterations in this process
Quality of SAP+ and responsiveness and ability of CSP to resolve agency comments can create iterations in this process
Quality of SAR as well as number and types of risks can create iterations in this process
Certification Recommendation submitted to DSAWG for comment then to DISA AO for authorization

Content

- Initiation
  - CSP submits SSP+
  - DISA assigns Certifying Authority (CA) and Holds CSP Kick-Off
- System Security Plan Review
  - CA review of SSP
  - CSP addresses CA concerns
- Security Assessment Planning (SAP)
- 3rd Party Assessment Organization (3PAO) creates SAP and CA reviews
- CSP addresses CA concerns
- Testing – 3PAO tests and creates Security Assessment Report (SAR)
- SAR Review Meeting
  - CA reviews SAR
  - CSP addresses CA concerns and creates Plan of action and Milestones (POAM)
- DSAWG Review – DSAWG comments on documentation
- Authorize – Final AO Review/PA Memo Sign Off
- Added to DISA Cloud Service Catalog

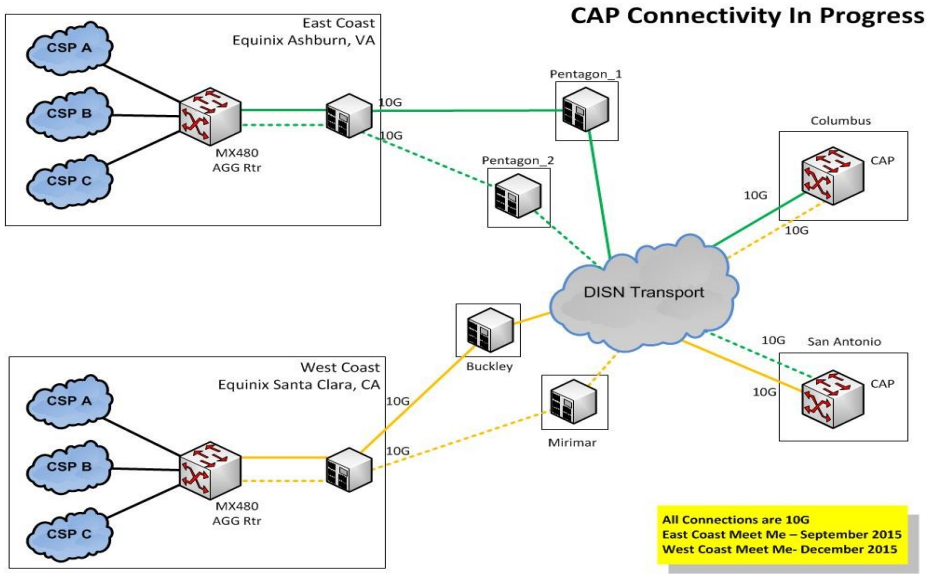
Cloud Access Point

Topic

Cloud Access Point (CAP)

You should be able to:

Questions



Content

- All CSOs at Information Impact Level 4 or higher are required to be connected to the DISN through a DOD CIO approved Cloud Access Point (CAP)
- A CAP can be provided by DISA or a DOD Component
- The processes for connecting to the DISA CAP or implementing a DOD Component CAP are still in development.
- As DOD strives to meet the objectives of the DOD CIO to maximize the use of cloud computing, the DOD must protect the DODIN against cyber threats.
- DISA is responsible for developing the requirements and implementing a CAP to provide DODIN perimeter protection at the connection point to CSO that would include side channel attacks from the CSO to reach the DODIN.
- The purpose of the CAP is to provide a barrier of protection between the DOD and the CSP IT infrastructure.
- The CAP will prevent attacks against the DODIN infrastructure and mission applications that originate in the Cloud Service Environment.
- It will provide a consistent level of security that facilitates the implementation of commercial and DOD provided cloud services to support DOD mission applications. The CAP will provide the ability to detect and prevent an attack before reaching the DODIN.
- DoD O-8530.1-M DoD, Computer Network Defense (CND) Service Provider Certification and Accreditation Process requires all DoD information systems to be supported by a certified CND Provider.

Authorizing Official Tasks

Topic

Authorizing Official Tasks

You should be able to:

Questions

Content

- Categorize system/application Information Impact Level
- Identify CSP Offering(s) with DoD Provisional Authorizations (PAs) that meet Information Impact Level
- Review existing CSO security documentation and determine additional mission security controls, testing, and assessment required for mission requirements
- Maximize use of existing body of evidence (e.g. scope, testing, results, residual risk, POA&Ms, continuous monitoring data) for the CSO
- Identify and resolve any additional testing requirements to assess the complete IT infrastructure supporting the mission
- Conduct testing and assessment of risks and vulnerabilities
- Document results of testing and assessment in Security Assessment Report and security Plan of Action and Milestones (POA&M) to mitigate security risks
- Prepare Security Authorization Package (SAP) for AO
- AO review of SAP
- If risk is acceptable – issue an Approval to Operate (ATO), explicitly reflecting acceptance of risk and liabilities identified in the assessments, for the Mission Owner's unique system and mission.
- If risk is not acceptable – issue a Denial of Approval to Operate (DATO) and indicate risks that are required to be mitigated to obtain ATO

Security A&A Risk Terms

Topic

Security A& A Risk Terms

You should be able to:

Match key terms to their definitions

Questions

Match key terms to their definitions

Content

- **Authorizing Official** – as described in DoD Risk Management Framework (RMF)means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations organizational assets, individuals, other organizations, and the Nation.
- **Cloud Access Point (CAP)** – a DoD system of network boundary protections and monitoring devices through which cloud services outside the DoD security boundary must traverse to connect to resources inside the DoD security boundary
- **Controlled Unclassified Information (CUI)** – established by Executive Order 13556 in November 2010, this is the categorical designation of unclassified information that under law or policy requires protection from unauthorized disclosure.
- **DoD Provisional Authorization (PA)** – is an acceptance of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DoD networks
- **FedRAMP** - The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The Office of Management and Budget (OMB) mandates compliance with FedRAMP for all Federal Agencies as their systems and applications are migrated to the commercial cloud under the Federal Government's Cloud-First initiatives.

Security A&A Risk Terms (Continued)

Topic

Security A& A Risk Terms

You should be able to:

Questions

Content

- **Impact Levels** – Cloud security information impact levels are defined by the combination of:
  - the sensitivity of information to be stored and processed in the CSP environment
  - the potential impact of an event that results in the loss of confidentiality, integrity or availability of that information.
  - Information Impact Levels consider the potential impact should the confidentiality or the integrity of the information be compromised
  - DoD Mission Owners categorize mission information systems in accordance with policy (DoDI 8510.01 and CNSSI 1253) to identify the impact level that most closely aligns with the defined categorization and information sensitivity.
- **Joint Authorization Board (JAB)** - The Joint Authorization Board (JAB) members are the CIOs from DHS, GSA, and DoD. The JAB defines and establishes the FedRAMP baseline system security controls and the accreditation criteria for Independent Assessors (3PAOs). The JAB works closely with the FedRAMP PMO to ensure that FedRAMP baseline security controls are incorporated into consistent and repeatable processes for security assessment and authorizations of CSPs. The JAB also issues provisional authorizations for cloud services they believe will be leveraged the most government wide.
- **Multi-Tenancy** – A design principle allowing a single instance of a computing resource to provide separate environments to serve multiple client organizations

Security A&A Risk Terms (Continued)

Topic

Security A&A Risk Terms

You should be able to:

Questions

Content

- **Personally Identifiable Information (PII)** — any information about an individual maintained by an agency
  - (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records
  - (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
- **Physical Separation** – isolation of resources is provided by hardware controls or tangible means (e.g., an "air gap"). Note: used more with regard to separation of infrastructure within a facility
- **Public Cloud** – A cloud deployment model in which the cloud infrastructure is made available to the general public or large industry group, and is owned by an organization selling cloud services.
- **Security Authorization Package (SAP)** – contains the security testing artifacts, Security Assessment Report (SAP), Plan of Action and Milestones (POA&M) to mitigate any security risks found, and any Provisional Authorization packages needed by the AO to determine whether to approve a system going into production and process DoD data in support of Component missions.

Recapitulation of Modules – 1, 2, 3, 4

Topic

Review Previous Content

Content

You should be able to:

Questions

Module 5 - Review

Topic

Summary

Content

You should be able to:

Questions

Module 5 – Summary Questions

Topic

Summary

Content

You should be able to:

Questions

Information Impact Level

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	DEPLOYMENT MODELS	PERSONNEL REQUIREMENTS
1	----------Impact Level Deprecated----------					
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	PUBLIC	National Agency Check and Inquiries (NACI)
3	----------Impact Level Deprecated----------					
4	CUI or Non-CUI Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	Favorably Adjudicated SSBI SECRET Clearance NDA

Information Impact Levels

- **Level 1**: Level 1 is no longer used and has been merged with Level 2.
- **Level 2**: Non-Controlled Unclassified Information (CUI), Level 2 includes all data cleared for public release, as well as some DoD private unclassified information not designated as CUI or critical mission data, but the information requires some minimal level of access control. This level accommodates Non-CUI information categorizations based on CNSSI-1253 up to low confidentiality and moderate integrity (L-M-x).
- **Level 3**: Level 3 is no longer used and has been merged with Level 4.
- **Level 4**: Controlled Unclassified Information, Level 4 accommodates CUI which is the categorical designation that refers to unclassified information that under law or policy requires protection from unauthorized disclosure as established by Executive Order (EO) 13556, Controlled Unclassified Information (November 2010) or other mission critical data. Designating information as CUI or critical mission data to be protected at Level 4 is the responsibility of the owning organization. Determination of the appropriate impact level for a specific mission with CUI and mission data will be the responsibility of the mission AO. Some types of CUI may not be eligible to be hosted on Impact Level 4 and 5 CSOs without a specific rider to the DoD PA. (e.g. for Privacy.) This level accommodates CUI information categorizations based on CNSSI-1253 up to moderate confidentiality and moderate integrity (M-M-x)
- **Level 5**: Controlled Unclassified Information, Level 5 accommodates CUI that requires a higher level of protection than that afforded by Level 4 as deemed necessary by the information owner, public law, or other government regulations. Level 5 also supports unclassified National Security Systems (NSSs) due to the inclusion of NSS specific requirements in the FedRAMP+ C/CEs. As such, NSS must be implemented at Level 5. Some types of CUI may not be eligible to be hosted on Impact Level 4 and 5 CSOs without a specific rider to the DoD PA (e.g. for Privacy.) This level accommodates NSS and CUI information categorizations based on CNSSI-1253 up to moderate

Source: Draft DoD Cloud Computing Security Requirements Guide V1 R2

Examples of Controlled Unclassified Information

- **Export Control-**--Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
- **Privacy Information-**--Refers to personal information or, in some cases, personally identifiable information (PII) as defined in Office of Management and Budget (OMB) M-07-16 or means of identification as defined in 18 USC 1028(d)(7) .
- **Protected Health Information (PHI)** as defined in the Health Insurance Portability and Accountability (HIPAA) Act of 1996 (Public Law (PL) 104-191) .
- **Other** information requiring explicit CUI designation (i.e., For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information).